03-06-00 A

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. **US 008002** Total Pages 25

First Named Inventor or Application Identifier

Fleming et al

Express Mail Label No. EJ 903756252 US

Date of Deposit **3 March 3000**

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. ☒ Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)
2. ☒ Specification *Total Pages* 15
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings *(if filed)*
- Detailed Description
- Claim(s)
- Abstract of the Disclosure
3. ☒ Drawings *(35 USC 113) Total Sheets* 1
4. ☒ Oath or Declaration *Total Pages 4*
a. ☒ Newly executed (original or copy)
b. ☐ Copy from a prior application (37 CFR 1.63(d))
(for continuation/divisional with Box 17 completed)
[Note Box 5 below]
i. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation By Reference
(useable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. ☐ Microfiche Computer Program *(Appendix)*
7. ☐ Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. ☐ Computer Readable Copy
b. ☐ Paper Copy (identical to computer copy)
c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. ☒ Assignment Papers (cover sheet & document(s))
9. ☐ 37 CFR 3.73(b) Statement (when there is an assignee) ☐ Power of Attorney
10. ☐ English Translation Document (if applicable)
11. ☐ Information Disclosure Statement (IDS)/PTO 1449 ☐ Copies of IDS Citations
12. ☐ Preliminary Amendment
13. ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
14. ☐ Small Entity Statement(s) ☐ Statement filed in Prior Application, Status still proper and desired.
15. ☐ Certified Copy of Priority Document(s)
(if foreign priority is claimed)
16. ☒ Other
☒ Check in the amount of **$730**
☐ .

17. If a CONTINUING APPLICATION, *check appropriate box and supply the requisite information:*
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No:

18. CORRESPONDENCE ADDRESS: **Corporate Patent Counsel**
U.S. Philips Corporation
580 White Plains Road
Tarrytown, N.Y. 10591

19. Certificate of Express Mail:
I hereby certify that this paper and the items identified above are being deposited with the U.S. Postal Service "Express Mail Post Office to Addresses" service under 37 C.F.R. Section 1.10 on the 'Date of Deposit', indicated above, and is addressed to: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

Robert M. McDermott, Registration Number 41,508

IEEE 1394 Link Layer Chip with "5C" Authentication and Key Exchange Accelerator

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to the field of communications, and in particular to secure communications via an IEEE 1394 (firewire) interface.

2. Description of Related Art

Secure communications between and among devices is becoming increasingly important for the protection of copyright material and other communiqués. An organization known as the Digital Transmission Licensing Authority (DTLA) has created the Digital Transmission Content Protection Specification, commonly known as the "5C" specification. The 5C specification defines a cryptographic system comprising a number of cryptographic components, including methods for enciphering and deciphering content material, and methods for determining secure cryptographic keys for use in this enciphering and deciphering of the content material.

A commonly used protocol for the transmission of audio/visual material among audio/visual applications is the IEEE 1394 protocol and interface. Special purpose controllers have been developed to support the transfer of enciphered material between an application program and the IEEE 1394 bus interface, including the enciphering and deciphering of the content material being transferred in accordance with the 5C specification, based on cryptographic keys that are provided by the application program. As is known in the art, given a sufficiently robust key, the enciphering and deciphering of information can provide a high level of security, and can be effected with relatively little overhead, being based primarily on a "shift and add" or similar operation. The complexity required to generate the keys that are used to perform the enciphering and deciphering, on the other hand, is substantial. To minimize the potential damage caused by a breach of security of keys, the 5C specification calls for the generation of unique keys by the devices involved in the transfer of the information. A discovery of the keys that are used by one pair of devices provides no information concerning the keys used by another pair of devices. When a communication of protected information is required, the devices generate a unique set of keys for ciphering and deciphering the information. The generation of unique keys for each

session of information transfer is effected via a "key exchange", which is an exchange of parameters that are used to generate keys within each device.

In the 5C specification, an elliptic curve Diffie-Hellman key exchange, and an elliptic curve Digital Signature algorithm is specified for full authentication. The elliptic curve computations are known in the art, and are mathematically complex. For sufficient security, the computations use relatively large numbers, in the order of 160 or more bits. The 5C specification requires that these operations be completed in a limited amount of time, for operation effectiveness, as well as security reasons. Because of the mathematical complexity and required efficiency, a conventional implementation of these tasks includes a software program that is executed on a high-performance microprocessor. For example, on a home computer system with an IEEE 1394 interface, the application program that is used to transfer the information to other devices contains the sub-programs that compute or verify digital signatures, and, if the signatures are verified, effect a key exchange. These sub-programs are typically run on a Pentium® or similar high performance processor, via, for example, a "C" program that includes complex operations that are known to be computationally irreversible. That is, a knowledge of the output of the complex operation provides little or no information regarding the parameters that were used to generate the output. For example, in the context of the 5C specification, elliptic curve cryptography is based on a determination of a point on an elliptic curve based on another point on the curve.

As the name "key exchange" implies, both the device that will be transmitting the protected information, and the device that will be receiving the protected information must participate in this exchange, and therefore both devices must contain sufficient capabilities to effect the above described key exchange computations. Although the execution of a key exchange on a home computer is feasible, the cost of a high performance microprocessor can be prohibitive in many applications, specifically consumer electronic equipment, such as video recorders, CD players, and the like. Additionally, each application program on a computer, and each component device that is expected to comply with the 5C specification, must incur the cost of developing and testing, or purchasing and testing, the software required to effect the digital signing and key exchange tasks required by the 5C specification. As an alternative to a high-performance processor running a software program, a special purpose processor can be provided to facilitate the 5C authentication functions, but such a special purpose processor can be expected to require a

substantial modification to existing processing systems designs and architectures, and will add costs to each device that is expected to comply with the 5C specification.

BRIEF SUMMARY OF THE INVENTION

It is an object of this invention to facilitate the task of 5C authentication and key exchange. It is a further object of this invention to facilitate the task of 5C authentication and key exchange in an IEEE 1394 environment. It is a further object of this invention to minimize the burden on application programs for effecting authentication and key exchange. It is a further object of this invention to minimize the cost of implementing 5C authentication and key exchange in an IEEE 1394 environment. It is a further object of this invention to provide a device that facilitates 5C authentication and key exchange in existing system architectures.

These objects and others are achieved by incorporating authentication and key exchange functions, such as those conforming to the Digital Transmission Licensing Authority's (DTLA) Digital Transmission Content Protection (5C) Specification, into a link-layer access device of a conventional processing system. Because of the suitability of IEEE 1394 for transferring audio/video information, these functions are preferably embodied in an IEEE 1394 compatible link-layer access device. The link-layer access device of this invention is configured to support, for example, the elliptic curve multiplication functions of a Diffie-Hellman key exchange process, as well as digital signature generation and digital signature verification. By incorporating the authentication and key exchange functions into a link-layer access device, the system architecture and devices that are commonly used in conventional processing systems can be used, thereby providing an incremental path toward increased protection of copyright material. In a preferred embodiment, the conventional link-layer controller is configured to implement the authentication and key exchange processes, via calls to the link-layer access device to perform the complex mathematical operations, thereby eliminating the need for each application-layer program or device to implement these processes.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is explained in further detail, and by way of example, with reference to the accompanying drawings wherein:

FIG. 1 illustrates an example block diagram of a processing system in accordance with this invention.

FIG. 2 illustrates an example block diagram of a link-layer access device that facilitates cryptographic authentication and key exchange functions, including key exchange functions, in accordance with this invention.

Throughout the drawings, the same reference numerals indicate similar or corresponding features or functions.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 illustrates an example block diagram of a processing system 100 in accordance with this invention. By intent, the architecture of the processing system 100 is substantially identical to that of conventional prior-art processing systems. The processing system 100 includes an application device 110 that communicates with another device (not shown) via a physical-layer communications path, such as an IEEE 1394 bus 150. Consistent with common hierarchical protocol structures, the application device 110 transfers information to the physical-layer communications path via a link-layer access device 200 and a physical-layer access device 130. A node controller 120 manages the flow of information between the application device 110 and the link-layer access device 200, and the processing of information at the link-layer access device 200.

In accordance with this invention, the link-layer access device 200 includes an authentication and key exchange accelerator 250, as illustrated in FIG. 2. The authentication and key exchange accelerator 250 facilitates cryptographic tasks, such as key exchange, digital signing, and digital signature verification. Copending U.S. patent application, "Simple Algorithmic Cryptography Engine", U.S. serial number 09/466,392, filed 17 December 1999 for George Fleming, Farrell Ostler, and Antoine Dagher, provides a processing architecture that is particularly well suited for cryptographic processing, and is incorporated by reference herein. In the copending application, a variety of techniques are employed to minimize the complexity of the design and to minimize the complexity of the interconnections within the device, thereby allowing

the engine to be incorporated within an existing link-layer access device integrated circuit design. A variety of techniques are also employed to ease the task of programming the processor for cryptographic processes, and to optimize the efficiency of instructions that are expected to be required for effecting digital signing, verification, and key exchange. Because authentication and key exchange tasks are characterized by operations on wide data items, particular emphasis is placed on the efficient processing of multi-word operations, including the use of constants having the same width as an instruction word. A simplified arithmetic unit is provided that is specifically designed to support digital signing, verification and key exchange, with minimal overhead.

In a preferred embodiment of this invention, the link-layer access device 200 receives commands from the node controller 120 to effect the provided authentication and key exchange tasks. As is common in the art, the controller 120 is typically a low-cost microprocessor, such as an 8051-type controller, with insufficient processing power to provide the authentication and key exchange tasks. By providing the authentication and key exchange accelerator 250 in the link-layer access device 200, to which the node controller 120 is traditionally coupled, the authentication and key exchange tasks can be off-loaded from the application device 110 without introducing a change to the traditional processing system architecture. Preferably, the link-layer access device 200 of this invention has the same pin-out of prior art link-layer access devices, so that existing processing system designs can be upgraded to include authentication and key exchange capabilities via changes to the software and/or firmware used in the node controller 120. The resultant combination of node controller 120 and link-layer access device 200 substantially eliminates the need for application devices 110, and corresponding application-layer programs, to include the complex operations required to effect digital signing, verification, and key exchange, thereby minimizing the development time and cost for introducing DTLA 5C security to copy protected material.

The node controller 120 is configured to control the sequences involved in authentication and key exchange processes, and to provide cryptographic parameters and commands to the link-layer access device 200, as required, via the controller interface 220 of the link-layer access device 200. The authentication and key exchange accelerator 250 of the link-layer access device 200 is configured to perform the complex mathematical operations required to produce cryptographic items to fulfill each command, based on the parameters provided by the controller 120 or stored

within the link-layer access device 200. For ease of reference, the terms cryptographic items and parameters are used herein to include the parameters, arguments, intermediate results, final results, and so on, that are communicated among and between devices for the purpose of effecting a task related to cryptography, such as digital signing, verification, and key exchange and generation. In a preferred embodiment, the link-layer access device 200 is configured to perform the following operations, in response to corresponding commands from the node controller 120:

Basepoint Multiply	(first phase of Diffie-Hellman key exchange)
Point Multiply	(final phase of Diffie-Hellman key exchange)
EC-DSA Verify	(verify digital signature of a message)
EC-DSA Sign	(digitally sign a message),

where EC-DSA corresponds to the Elliptic-Curve Digital Signature Algorithm, common in the art. The basepoint multiply and point multiply operations include the aforementioned elliptic curve multiplication operations that provide a point on an elliptic curve based on another point on the curve and one or more parameters associated with the elliptic curve Diffie-Hellman key exchange algorithm, common in the art. The EC-DSA verify operation verifies a source of a message from another device, based on a key associated with the other device. The EC-DSA sign operation binds a cryptographic item to the message, to facilitate a subsequent verification of the source of the message at another device, based on a key associated with this device.

In a Diffie-Hellman key exchange, each device chooses a local parameter, such as a large random number, and computes a particular function with this parameter as an argument. The result of this function is communicated to the other device. Each device then computes a second function with the communicated item and its local parameter as arguments. The two functions that are applied in this exchange are such that the result provided by the second function in each device is identical, and also such that knowledge of the communicated items provides no assistance to a third party in determining the common result. For example, consider x and y being the local parameters of each device, and the result of a modular exponentiation of a commonly known integer g by the local parameter x, y ($X = g^x \bmod m$; $Y = g^y \bmod m$) being the communicated items X and Y, where m is also commonly known to each device. Each device computes a second modular exponentiation of the received item ($K1 = Y^x \bmod m$; $K2 = X^y \bmod m$). Both K1 and K2 will be equal to $g^{xy} \bmod m$ ($K1 = (g^y \bmod m)^x \bmod m$; $K2 = (g^x \bmod m)^y$

mod m), and, provided that x, and y are large, a knowledge of g, m, X, and Y provides little or no assistance in determining the value g^{xy} mod m. This common result of the second function (g^{xy} mod m) at each device is used as the key for ciphering and deciphering messages. In an embodiment that satisfies the 5C specification, the functions are elliptic curve functions, rather than exponentiation functions, although this invention is not, per se, limited to the 5C specification or elliptic curve functions. In a preferred embodiment, the link-layer access device 200 facilitates the authentication processes of signing and verifying, as well as key exchange, by providing operations that are commonly used in cryptographic applications, such as exponentiation or elliptic curve multiplications, and are too complex for embodiment in a low-cost microcontroller 120. The microcontroller 120 in this preferred embodiment, on the other hand, controls the sequence of operations, the communication of parameters with the link-layer access device 200, and so on, to effect the appropriate authentication and key exchange tasks.

The link-layer access device 200 of this invention includes the components required to perform conventional link-layer access operations, thereby providing the aforementioned authentication and key exchange operations at a minimal incremental cost compared to conventional processing system. The link-layer access device 200 includes an application-layer interface 210 that provides the communications interface with the application device, or devices, 110 of FIG. 1, and a physical-layer interface 230 that provides the communications interface with the physical-layer device, or devices, 130. Conventional control and status registers 260 are used to facilitate the interaction of the link-layer access device 200 with the physical and application layer devices via the appropriate interface 230, 210. For example, the 1394 protocol supports both isochronous and asynchronous communications. The isochronous, or "real-time", data must be placed on, and removed from, the 1394 bus 150 at specific intervals, to achieve, for example video renderings at a specific frame rate. Asynchronous communications are achieved by communicating data whenever the bus 150 is available. The transmit/receiver buffer 240, as its name implies, buffers the data received from either domain, as required. As shown, for completeness, the link-layer access device 200 may include an optional cipher/decipher device 245 that ciphers or deciphers the information being transferred through the buffer 240. The key that is used for this cipher/decipher operation is provided to the device 245 by the node controller 120, via the controller interface 220, after the aforementioned key exchange process is completed.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the invention and are thus within its spirit and scope. For example, the invention has been presented using the paradigm of DTLA 5C authentication and key exchange tasks in an IEEE 1394 environment. Although the details of this invention are particularly well suited for DTLA 5C authentication and key exchange and IEEE 1394 communications, one of ordinary skill in the art will recognize the suitability of this invention to other security schemes, and other communications protocols. In like manner, the authentication and key exchange accelerator 250 has been presented as supporting four operations that facilitate cryptographic operations, although fewer or more operations may be supported, depending upon the circuit area in the link-layer access device 200 that can be devoted to cryptographic tasks. For example, random number generation, hashing, and the like can be added to the link-layer access device 200, if the required circuit area for these functions is available. These and other system configuration and optimization features will be evident to one of ordinary skill in the art in view of this disclosure, and are included within the scope of the following claims.

CLAIMS

We claim:

1. A processing system comprising:

an application device that is configured to communicate information with a physical-layer access device via a link-layer access device,

a node controller that is configured to control the link-layer access device,

the link-layer access device, operably coupled to the application device, the node controller, and the physical-layer access device, that is configured to facilitate an exchange of the information from and to the application device with data that is communicated to and from the physical-layer access device;

wherein,

the link-layer access device is further configured to provide, in response to one or more commands from the node controller, one or more cryptographic items based on one or more parameters from the node controller.

2. The processing system of claim 1, wherein

the one or more cryptographic items include at least one of:

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

3. The processing system of claim 1, wherein

the one or more cryptographic items include:

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

4. The processing system of claim 1, wherein

the link-layer access device includes a multiplication device that is configured to derive a second point on an elliptic curve from a first point on the elliptic curve, based on the one or more of the parameters from the node controller.

5. The processing system of claim 1, wherein

the node controller is configured to effect an exchange of a cryptographic key with an other processing system, and

the one or more cryptographic items from the link-layer access device includes the cryptographic key.

6. The processing system of claim 1, wherein

the commands from the node controller include: a basepoint multiply command, a point multiply command, an EC-DSA verify command, and an EC-DSA sign command.

7. A link-layer access device comprising:

an application-layer interface device that is configured to communicate information with an application-layer device,

a physical-layer interface device that is configured to communicate data with a physical-layer device,

a buffer device, operably coupled to the application-layer interface device and the physical-layer interface device, that is configured to facilitate an exchange of the information of the application-layer device and the data of the physical-layer device,

a controller interface device, operably coupled to the application-layer interface device and the physical-layer interface device, that is configured to facilitate control of the exchange of information and data, and

an accelerator, operably coupled to a controller via the controller interface device, that is configured to compute one or more cryptographic items, in response to one or more cryptographic commands from the controller, and to thereafter communicate the one or more cryptographic items to the controller.

8. The link-layer access device of claim 7, wherein

the accelerator includes a multiplication device that is configured to derive a second point on an elliptic curve from a first point on the elliptic curve, based on one or more of parameters provided by the controller.

9. The link-layer access device of claim 7, wherein

the one or more cryptographic items includes at least one of:

a signature of a message,

a verification of a digital signature,

a hash of one or more parameters,

a random number,

an exponentiation of one or more parameters, and

an elliptic curve multiplication of one or more parameters,

the one or more parameters being provided by the controller.

10. The link-layer access device of claim 7, wherein

the one or more cryptographic items include:

a signature of a message,

a verification of a digital signature, and

an elliptic curve multiplication of one or more parameters,

the one or more parameters being provided by the controller.

11. The link-layer access device of claim 7, wherein

the one or more cryptographic commands include: a basepoint multiply command, a point multiply command, an EC-DSA Verify command, and an EC-DSA sign command.

12. A method for communications comprising:

communicating information from and to an application device to and from a physical-layer access device via a link-layer access device,

controlling the link-layer access device, in dependence upon commands from a node controller,

effecting an exchange of the information from and to the application device with data that is communicated to and from the physical-layer access device, and

determining one or more cryptographic items via computations within the link-layer access device, based on one or more parameters that are provided to the link-layer access device by the node controller.

13. The method of claim 12, wherein

the one or more cryptographic items include at least one of:

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

14. The method of claim 12, wherein

the one or more cryptographic items include:

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

15. The method of claim 12, wherein

determining the one or more cryptographic items includes

deriving a second point on an elliptic curve from a first point on the elliptic curve, based on the one or more of the parameters from the node controller.

15. The method of claim 12, further including

effecting an exchange of a cryptographic key with an other processing system, wherein

the one or more cryptographic items from the link-layer access device includes the cryptographic key.

16. The method of claim 12, wherein

the commands from the node controller include: a basepoint multiply command, a point multiply command, an EC-DSA verify command, and an EC-DSA sign command.

IEEE 1394 Link Layer Chip with "5C" Authentication and Key Exchange Accelerator

ABSTRACT OF THE DISCLOSURE

Authentication and key exchange functions, such as those conforming to the Digital Transmission Licensing Authority's (DTLA) Digital Transmission Content Protection (5C) Specification, are incorporated into a link-layer access device of a conventional processing system. Because of the suitability of IEEE 1394 for transferring audio/video information, these functions are preferably embodied in an IEEE 1394 compatible link-layer access device. The link-layer access device of this invention is configured to support, for example, the elliptic curve multiplication functions of a Diffie-Hellman key exchange process, as well as digital signature generation and digital signature verification. By incorporating the authentication and key exchange functions into a link-layer access device, the system architecture and devices that are commonly used in conventional processing systems can be used, thereby providing an incremental path toward increased protection of copyright material. In a preferred embodiment, the conventional link-layer controller is configured to implement the authentication and key exchange processes, via calls to the link-layer access device to perform the complex mathematical operations, thereby eliminating the need for each application-layer program or device to implement these processes.

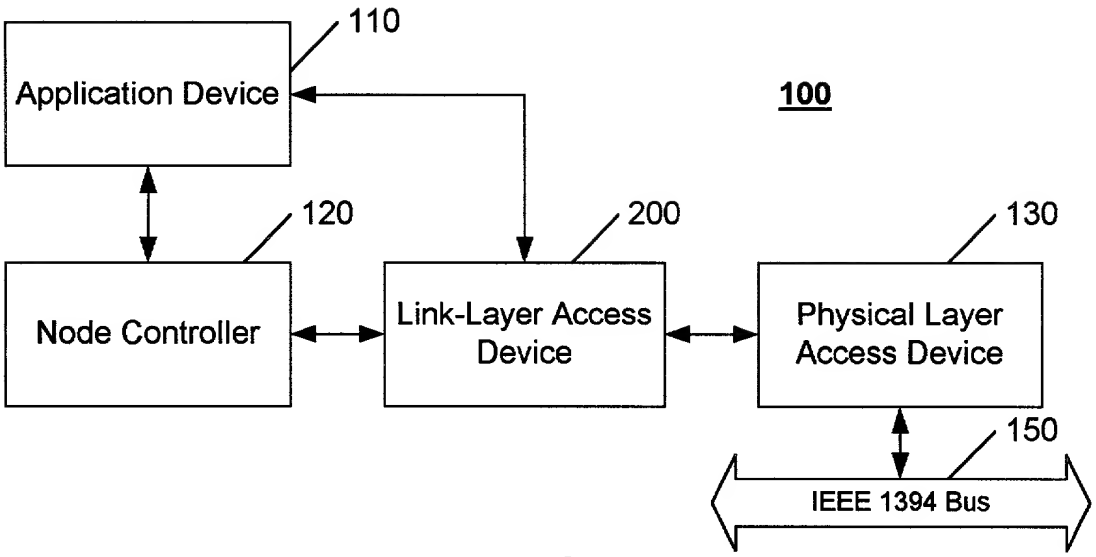
110
Application Device
100
120
200
130
Node Controller
Link-Layer Access Device
Physical Layer Access Device
150
IEEE 1394 Bus

FIG. 1

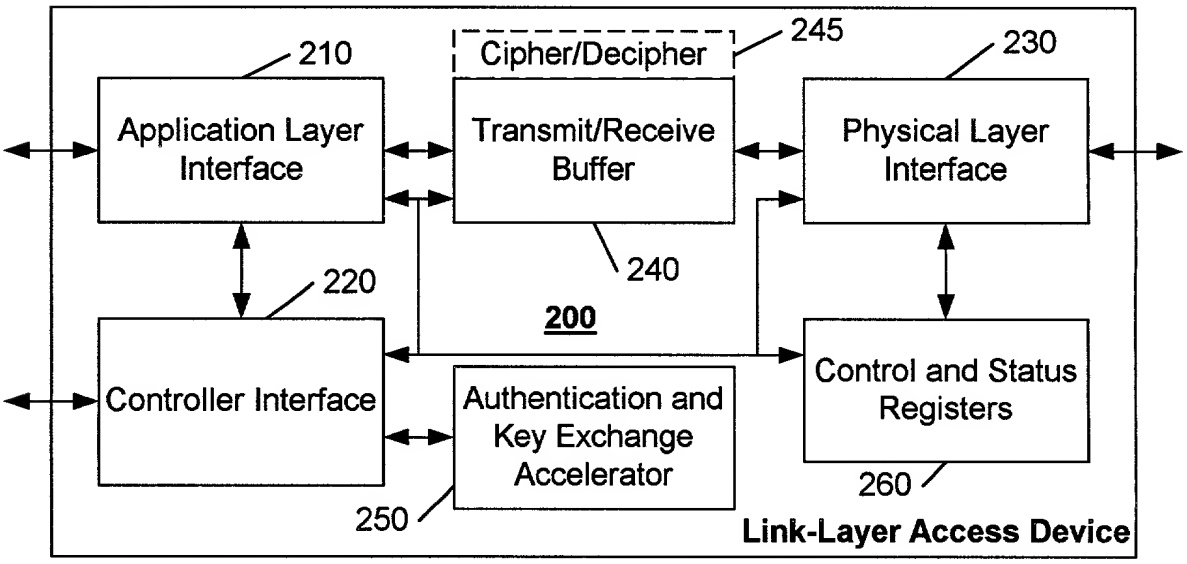
210
Cipher/Decipher
245
230
Application Layer Interface
Transmit/Receive Buffer
Physical Layer Interface
240
220
200
Controller Interface
Authentication and Key Exchange Accelerator
Control and Status Registers
260
250
Link-Layer Access Device

FIG. 2

DECLARATION and POWER OF ATTORNEY

Attorney's Docket No. **US 008002**

As a below named inventor, I hereby declare that:
My residence, post office address and citizenship are as stated below next to my name.
I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **IEEE 1394 LINK LAYER CHIP WITH "5C" AUTHENTICATION AND KEY EXCHANGE ACCELERATOR** the specification of which (check one)

X is attached hereto.
__ was filed on as Application Serial No. _ and was amended on _____ (if applicable).
I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by the amendment(s) referred to above.
I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulation, §1.56(a).
I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

COUNTRY	APPLICATION NUMBER	DATE OF FILING (DAY, MONTH, YEAR)	PRIORITY CLAIMED UNDER 35 U.S.C. 119

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application (s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35 United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

PRIOR UNITED STATES APPLICATION(S)

APPLICATION SERIAL NUMBER	FILING DATE	STATUS (PATENTED, PENDING, ABANDONED)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)
Algy Tamoshunas, Reg. No. 27,677
Jack E. Haken, Reg. No. 26,902

SEND CORRESPONDENCE TO:	DIRECT TELEPHONE CALLS TO:
Corporate Patent Counsel; U.S. Philips Corporation; 580 White Plains Road; Tarrytown, NY 10591	Robert J. Kraus, Reg. 26.358 (914) 333-9634

Dated: 2nd March 2000		Inventor's Signature: GFleming		
Full Name of Inventor	Last Name **Fleming**	First Name **George**	Middle Name	
Residence & Citizenship	City **Hampshire**	State or Foreign Country **United Kingdom**	Country of Citizenship **U.K.**	
Post Office	Street **Oak Cottage, Slab Lane**	City **Hampshire**	State or Country	Zip Code

s:\kr\Catalog2

Address	West Wellow Romsey		U.K.	SO51 6BY

Dated: 2ND MARCH 2000		Inventor's Signature: Bruce Murray		
Full Name of Inventor	Last Name Murray	First Name Bruce	Middle Name	
Residence & Citizenship	City Hampshire	State or Foreign Country United Kingdom	Country of Citizenship U.K.	
Post Office Address	Street 12 Noyce Drive Fair Oak Eastleigh	City Hampshire	State or Country U.K.	Zip Code SO50 7LT

Dated:		Inventor's Signature:		
Full Name of Inventor	Last Name Tolsch	First Name Don	Middle Name	
Residence & Citizenship	City Albuquerque	State or Foreign Country NM	Country of Citizenship U.S.	
Post Office Address	Street 5836 Lost Dutchman NE	City Albuquerque	State or Country U.S.A.	Zip Code 87111

Dated:		Inventor's Signature:		
Full Name of Inventor	Last Name	First Name	Middle Name	
Residence & Citizenship	City	State or Foreign Country	Country of Citizenship	
Post Office Address	Street	City	State or Country	Zip Code

s:\kr\Catalog2

DECLARATION and POWER OF ATTORNEY

Attorney's Docket No. US 008002

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **IEEE 1394 LINK LAYER CHIP WITH "5C" AUTHENTICATION AND KEY EXCHANGE ACCELERATOR** the specification of which (check one)

X is attached hereto.

___ was filed on as Application Serial No. _ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by the amendment(s) referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulation, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

COUNTRY	APPLICATION NUMBER	DATE OF FILING (DAY, MONTH, YEAR)	PRIORITY CLAIMED UNDER 35 U.S.C. 119

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application (s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35 United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

PRIOR UNITED STATES APPLICATION(S)

APPLICATION SERIAL NUMBER	FILING DATE	STATUS (PATENTED, PENDING, ABANDONED)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

Algy Tamoshunas, Reg. No. 27,677

Jack E. Haken, Reg. No. 26,902

SEND CORRESPONDENCE TO:	DIRECT TELEPHONE CALLS TO:
Corporate Patent Counsel; U.S. Philips Corporation; 580 White Plains Road; Tarrytown, NY 10591	Robert J. Kraus, Reg. 26,358 (914) 333-9634

Dated:		Inventor's Signature:		
Full Name of Inventor	Last Name **Fleming**	First Name **George**	Middle Name	
Residence & Citizenship	City **Hampshire**	State or Foreign Country **United Kingdom**	Country of Citizenship **U.K.**	
Post Office Address	Street **Oak Cottage, Slab Lane West Wello Romsey**	City **Hampshire**	State or Country **U.K.**	Zip Code **SO51 6BY**

s:\kr\Catalog2

Dated:		Inventor's Signature:		
Full Name of Inventor	Last Name **Murray**	First Name **Bruce**	Middle Name	
Residence & Citizenship	City **Hampshire**	State or Foreign Country **United Kingdom**	Country of Citizenship **U.K.**	
Post Office Address	Street **12 Noyce Drive Fair Oak Eastleigh**	City **Hampshire**	State or Country **U.K.**	Zip Code **SO50 7LT**

Dated: 3/2/00		Inventor's Signature:		
Full Name of Inventor	Last Name **Tolsch**	First Name **Don**	Middle Name	
Residence & Citizenship	City **Albuquerque**	State or Foreign Country **NM**	Country of Citizenship **U.S.**	
Post Office Address	Street **5836 Lost Dutchman NE**	City **Albuquerque**	State or Country **U.S.A.**	Zip Code **87111**

Dated:		Inventor's Signature:		
Full Name of Inventor	Last Name	First Name	Middle Name	
Residence & Citizenship	City	State or Foreign Country	Country of Citizenship	
Post Office Address	Street	City	State or Country	Zip Code

s:\kr\Catalog2